

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-115167

(43)Date of publication of application : 21.04.2000

(51)Int.Cl.

H04L 12/22

H04L 12/56

(21)Application number : 10-286508

(71)Applicant : NTT DATA CORP
DOWANGO:KK

(22)Date of filing : 08.10.1998

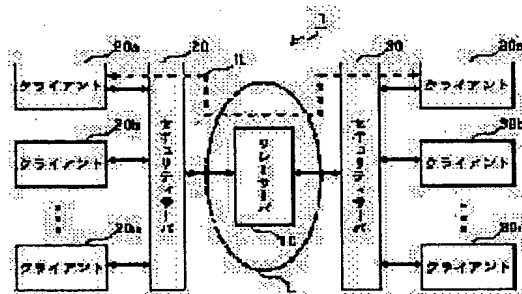
(72)Inventor : HIRAO YOSHIKUNI
KAWAKAMI KAZUO

(54) DATA COMMUNICATION METHOD, DATA REPEATER AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data communication system capable of performing real time communication even under the environment when direct data communication with an opposite side is limited.

SOLUTION: Between clients 20a-20n under security servers 20 and 30 for allowing the transmission of only the communication data of a prescribed form such as a firewall and the clients 30a-30n under the security server 30, a relay server 10 for relaying the communication data between the clients is provided. The relay server 10 performs the pseudo exchange of the communication data from the client 20a to a data form whose transmission is allowed by the security server 30 provided with the client 30a of a communicating opposite party as a subordinate and transmits it to the client 30a.



LEGAL STATUS

[Date of request for examination]

16.11.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

2998839

[Date of registration]

05.11.1999

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

Best Available Copy

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2000-115167

(P2000-115167A)

(43)公開日 平成12年4月21日(2000.4.21)

(51)Int.Cl.⁷

識別記号

FI

マークコード(参考)

H04L 12/22
12/56

H04L 11/26
11/20

5K030
102Z 9A001

審査請求 有 請求項の数10 OL (全10頁)

(21)出願番号

特願平10-286508

(22)出願日

平成10年10月8日(1998.10.8)

(71)出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(71)出願人 598138327

株式会社ダウンゴ
東京都中央区日本橋人形町2-14-6 セ
ルパ人形町

(72)発明者 平尾 吉邦

東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

(74)代理人 100099324

弁理士 鈴木 正剛

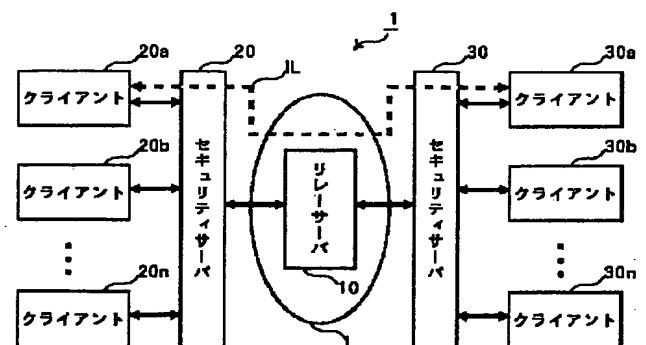
最終頁に続く

(54)【発明の名称】 データ通信方法、データ中継装置及び記録媒体

(57)【要約】

【課題】 相手側との間の直接的なデータ通信が制限される環境下においてもリアルタイム通信を行うことができるデータ通信システムを構築する。

【解決手段】 ファイアウォール等の所定形式の通信データのみの透過を許容するセキュリティサーバ20、30の配下にあるクライアント20a~20nと、セキュリティサーバ30の配下にあるクライアント30a~30nとの間に、クライアント間の通信データを中継するリレーサーバ10を設ける。このリレーサーバ10は、クライアント20aからの通信データを通信相手先のクライアント30aを配下にもつセキュリティサーバ30が透過を許容するデータ形態に擬似的に交換し、これをクライアント30a宛に送信する。



【特許請求の範囲】

【請求項1】 配下にある1又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、
外部装置から特定の前記通信装置宛に送信された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする、データ通信方法。

【請求項2】 前記外部装置、セキュリティ装置及び前記特定の通信装置をそれぞれ登録しておき、登録された外部装置から登録された通信装置宛の通信データのみの前記透過許容データに擬似的に変換して前記登録されたセキュリティ装置を透過させることを特徴とする、請求項1記載のデータ通信方法。

【請求項3】 それぞれ配下にある1又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容する複数のセキュリティ装置が介在する環境で行うデータ通信方法であって、
特定のセキュリティ装置の配下にある第1通信装置から他のセキュリティ装置の配下にある第2通信装置宛の通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させることを特徴とする、データ通信方法。

【請求項4】 前記通信データまたは透過許容データを前記第2通信装置毎に一時的に保持しておき、前記第2通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、前記透過許容データについてはそれを当該第2通信装置宛に送信することを特徴とする、請求項3記載のデータ通信方法。

【請求項5】 配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在し、
前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある相手側通信装置を登録する登録手段と、
前記登録された外部装置から前記登録された相手側通信装置宛の通信データを登録された前記セキュリティ装置用の透過許容データに変換するデータ変換手段と、
前記擬似的に変換された透過許容データの前記登録された相手側通信装置による取得を許容する手段とを備えて成る、データ中継装置。

【請求項6】 前記相手側通信装置毎のデータ記憶領域を有し、前記通信データ変換手段は、保持されている前記通信データを前記相手側通信装置からの要求を契機に前記透過許容データに擬似的に変換することを特徴とする、請求項5記載のデータ中継装置。

【請求項7】 前記データ変換手段は、前記通信データのヘッダ部分に、当該通信データが前記相手側通信装置

からの要求に応じたものであり且つHTTPまたはSMTPに従うデータである旨の情報を付加することで当該通信データを擬似的に前記透過許容データに変換することを特徴とする、

請求項6記載のデータ中継装置。

【請求項8】 前記外部装置が、前記セキュリティ装置と同種の機能を有する他のセキュリティ装置の配下にある通信装置であることを特徴とする、

請求項5記載のデータ中継装置。

【請求項9】 前記セキュリティ装置及び前記他のセキュリティ装置と共に、TCP/IPに準拠した公衆通信網に接続されることを特徴とする、

請求項8記載のデータ中継装置。

【請求項10】 配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも、
前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理と、

前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理と、

前記擬似的に変換された透過許容データの前記登録された相手側通信装置による取得を許容する処理とを実行させるためのプログラムが記録された、
コンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信装置間のデータ交換方法等に関し、特に、所定の通信形式の通信データのみの透過を許容するセキュリティ装置の配下にある通信装置と、外部装置、例えば他の独立したセキュリティ装置の配下にある通信装置との間で、ネットワーク上に配置されたデータ中継装置を介して行うデータ通信方法及びその関連技術に関する。

【0002】

【従来の技術】近年、インターネット等の不特定者が利用可能なネットワークを介してデータ通信を行う際のセキュリティ性を高めるために、当該ネットワークにセキュリティ装置を設けることが一般化している。この種のセキュリティ装置は、例えば配下にある通信装置とネットワークとの間に例えばファイアウォール等を設け、電子メールやホームページデータのような所定形態のデータのみの透過を許容し、それ以外のデータの透過を阻止する機能を有するものである。このようなセキュリティ装置において、インターネットにおけるサーバ機能を有するものは、セキュリティサーバと呼ばれている。

【0003】インターネットにこのようなセキュリティサーバを設けることは、配下の通信装置に対する不特定

者の有害なアクセスを排除し得る利点はあるが、以下のような問題も生じる。すなわち、ある通信装置と他の独立したセキュリティサーバの配下にある通信装置との間で、リアルタイム通信、例えば対戦型ゲームやリアルタイムチャットサービス等を行おうとしても、セキュリティサーバが介在するためにそれができない。すなわち、一方の通信装置から他方の通信装置に通信するためのセッション（論理回線路、以下同じ）を確立しようとしても、いずれかのセキュリティサーバ又は双方のセキュリティサーバによって、セッション確立が拒否されてしまう。これは、セキュリティサーバが、通信装置とネットワーク間のパケットを直接透過させずに間接経路でのみ透過を許容することで、配下の通信装置を保護しているためである。

【0004】そこで本発明は、相手側との間の直接的なデータ通信が制限される環境下においても、必要に応じてリアルタイム通信乃至それに近似した通信を行うことができる、改良されたデータ通信方法を提供することを課題とするものである。本発明の他の課題は、上記データ通信方法を実現するためのデータ中継装置、及び、上記データ通信方法をコンピュータ装置上で実行するための記録媒体を提供することにある。

【0005】

【課題を解決するための手段】上記課題を解決する本発明のデータ通信方法は、配下にある1又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、外部装置から特定の前記通信装置宛に送信された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする。好ましくは、前記セキュリティ装置及び前記特定の通信装置を予め登録しておき、登録した通信装置宛の通信データのみの前記透過許容データに擬似的に変換して登録されたセキュリティ装置を透過させるようにする。

【0006】前記セキュリティ装置が複数介在する環境でデータ通信を行う場合は、特定のセキュリティ装置の配下にある第1通信装置から他のセキュリティ装置の配下にある第2通信装置宛の通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させる。なお、前記通信データまたは透過許容データを前記第2通信装置毎に一時的に保持しておき、前記第2通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、前透過許容データについてはそれを当該第2通信装置宛に送信するようにしてもよい。

【0007】上記他の課題を解決する本発明のデータ中継装置は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外

部装置との間に介在するもので、前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある相手側通信装置を登録する登録手段と、前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に登録された前記セキュリティ装置用の透過許容データに変換するデータ変換手段と、前記擬似的に変換された透過許容データの登録された相手側通信装置による取得を許容する手段とを備えて構成したものである。

【0008】前記データ変換手段は、例えば、前記通信データのヘッダ部分に、当該通信データが前記相手側通信装置からの要求に応じたものであり且つHTTP (HyperText Transfer Protocol) またはSMTP (Simple Mail Transfer Protocol) に従うデータである旨の情報を付加することで当該通信データを擬似的に前記透過許容データに変換するように構成する。

【0009】上記他の課題を解決する本発明の記録媒体は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも下記の処理を実行させるためのプログラムが記録された、コンピュータ読取可能な記録媒体である。

(1) 前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理、

(2) 前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理、

(3) 前記擬似的に変換された透過許容データの登録された相手側通信装置による取得を許容する処理。

【0010】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。図1は、本発明を適用したデータ通信システムの概略構成図である。このデータ通信システム1は、セキュリティサーバ20の配下にある複数の通信装置（以下、通信装置を「クライアント」と称する）20a～20nと、他の独立したセキュリティサーバ30の配下にある複数のクライアント30a～30nを、インターネットL上のリレーサーバ10を介して双方向通信が可能な形態で接続して構成される。

【0011】セキュリティサーバ20、セキュリティサーバ30は、例えば次のような2つの条件を満たすデータのみの透過を許容する機能を備えた、公知のものである。

(1) ホームページへの接続に用いるHTTPまたは電子メールの交換に用いられるSMTPに従うデータであること、(2) 配下のクライアントから自サーバを通して外部ネットワーク、例えばインターネット上にあるホームページサーバにホームページデータを要求したとき

に、当該要求に応じてそのホームページサーバから返信されたデータであること。なお、本実施形態では、上記条件を満たす形態のデータを「透過許容データ」と称する。図1の参照符号1Lは、この透過許容データによって仮想的に形成される通信経路である。

【0012】通常、セキュリティサーバ20が、配下のクライアント20a～20nのいずれかとセキュリティサーバ30の配下のクライアント30a～30nのいずれかとの間でセッションを確立しようとしても、上記透過許容データ以外のデータの場合は、セキュリティサーバ30によってセッション確立が拒否される。そこで本実施形態では、リレーサーバ10で、データ通信を行うクライアント間に擬似的な透過許容データの通信経路1Lを形成し、リアルタイム通信またはそれに近似した通信を行えるようにする。

【0013】このような機能を実現するためのリレーサーバ10の機能ブロック構成を示したのが、図2である。このリレーサーバ10では、自サーバを介してデータ通信を行うクライアントの識別情報、各クライアントを配下にもつ（各クライアントを保護する）セキュリティサーバの識別情報、このセキュリティサーバによる上記透過許容データをデータベース部150へ登録しておく。例えば、クライアント20aがクライアント30aと通信を行う場合は、クライアント20a、クライアント30a、セキュリティサーバ20、セキュリティサーバ30の識別情報を登録しておく。

【0014】登録は、以下のようにして行う。例えばクライアント30aからクライアント30a宛のデータ送信要求が送信されたとする。リレーサーバ10は、このデータ送信要求をI/Oインターフェース110を介して受信し、登録・通信要求受付部120でこれを受け付けて判断処理部130に渡す。判断処理部130は、クライアント20aが登録が可能かどうかを調べ、可能であれば、ID発行部140に通知する。ID発行部140は、クライアント20a用にユニークなIDを発行し、これを識別情報としてデータベース部150へ登録する。また、クライアント20aを配下にもつセキュリティサーバ20について、既に識別情報や透過許容データが登録されているかどうかを調べ、未登録であれば、それらを登録する。

【0015】クライアント20a等が登録された場合は、クライアント20aの通信相手先となるクライアント30a及びこれを配下とするセキュリティサーバ30が登録されているかどうかを調べる。未登録の場合は上述の場合と同様の手順によってユニークなIDや透過許容データを登録する。クライアント30a等が登録された場合、あるいは既に登録されていた場合は、セッション確立部180でクライアント20aとクライアント30aとの間のセッションを確立する。

【0016】その後、クライアント20aから通信デー

タが送信されてきた場合は、これを登録・通信要求部120で受け付け、データ管理部170でクライアント毎に管理する。このとき、データ送信部160は、通信相手先のクライアント30aに当該クライアント宛の通信データがあることを通知する。クライアント30aから要求があった場合は、データ管理部170でセキュリティサーバ30の透過許容データに適合するようにデータを擬似的に変換し、そのデータをクライアント30a宛に送信する。

【0017】透過許容データへの擬似的な変換は、クライアント30a宛の通信データのヘッダ部に、例えば以下のような情報を付加することにより行う。

(1) その通信データがクライアント30aが要求したホームページサーバからの返信データである旨の情報、

(2) その通信データの形態が、セキュリティサーバ30の透過許容データ、例えば、ホームページデータ又は電子メールの形態である旨の情報。これにより、セキュリティサーバ30は、渡された通信データが、自サーバの配下にあるクライアント30aが要求したデータの返信であると認識するので、その通信データは排除されることなく、クライアント30aへ転送される。

【0018】なお、図示を省略したが、データ管理部170には、セッションが確立されたクライアント専用のバッファ領域がそれぞれ確保されており、各クライアントにとって、自分の記憶装置であるかのような取り扱いを可能にしている。例えば、クライアント20a用のバッファ領域に通信データを蓄積しておき、クライアント30aからの要求時にこれを読み出して随時透過許容データに擬似的に変換するような使用形態、クライアント30a用のバッファ領域に予め擬似的に透過許容データに変換したデータを格納しておき、クライアント30aがこれを随時読みとれるようにする使用形態、クライアント20aがクライアント30a用のバッファ領域に直接アクセスして通信データを蓄積し、クライアント30aからの要求を契機にこれを随時透過許容データに変換してクライアント30aへ送信する使用形態等が可能である。

【0019】上述のリレーサーバ10による各機能ブロック110～180は、通信機能を有するサーバ本体のCPU（プロセッサ）が、本発明の記録媒体に記録されたプログラムコードを読み取ることによって実現される。記録媒体は、通常、CPUが随時読み取り可能な固定型ディスクや半導体メモリであるが、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、DVD、磁気テープ等の可搬性メディア、あるいはコンピュータがアクセス可能なプログラムサーバ等に記録されて流通し、運用時に上記固定記録媒体にインストールされるものであってもよい。また、CPUが上記プログラムを実行することによって各機能ブロック110～180が形成されるだけでなく、その

プログラムの指示に基づいて当該サーバ本体上で稼働しているオペレーティングシステムが実際の処理の一部を行い、その処理を通じて上記各機能ブロック110～180が形成されるようにしてもよい。

【0020】次に、図3～図5を参照して上記リレーサーバ10の機能を説明する。まず、当事者となるクライアント20a、30a、これらを配下とするセキュリティサーバ20、30、各セキュリティサーバ20、30の透過許容データを予めリレーサーバ10に登録しておく必要がある。この場合の手順を示したのが図3である。すなわち、クライアント20aから、自己とセキュリティサーバ20の登録要求が発行されると（ステップS101）、リレーサーバ10は、その登録受付の可否を判断する。登録受付ができないときは、その旨をクライアント20aに通知する（ステップS102：No、S103）。登録可能なときは、登録要求を発行したクライアント専用のバッファ領域をデータ管理部170に確保し（ステップS102：Yes、S104）、クライアント/セキュリティサーバ用のIDを発行する（ステップS105）。そして、セキュリティサーバ20の透過許容データをデータベース部150に登録する（ステップS106）。

【0021】登録後は、図4及び図5に示す手順でデータ通信を開始する。図4において、クライアント20aからクライアント30aへのデータ送信要求が発行されると（ステップS201）、リレーサーバ10は、クライアント20a/セキュリティサーバ20が登録されており且つ適正なIDを所有しているか否かを調べる（ステップS202）。登録されていないければ拒絶を通知して初期状態に戻る（ステップS202：No、S203）。登録されている場合は、クライアント20a専用のバッファ領域を確保する（ステップS204）。その後、クライアント20aからの登録一覧送信要求を受け付け、クライアント20aに、登録済みのクライアントの一覧を通知する（ステップS204：Yes、S206）。

【0022】図5に移り、クライアント20aが、登録済みのクライアントの一覧から、クライアント30aが既に登録されていることを確認し、そのクライアント30aへのデータ送信要求を発行すると（ステップS301）、リレーサーバ10は、宛先であるクライアント30aが適正か否かを調べる（ステップS303）。適正でない場合は、データ通信ができない旨をクライアント20aに通知し、初期状態に戻る（ステップS303：No、S304）。適正であれば、クライアント30a専用のバッファ領域を確保するとともに、クライアント20aからデータ送信要求があった旨をクライアント30aへ通知する（ステップS305）。

【0023】その後、クライアント20aからの通信データを逐次受信し（ステップS306）、この受信した

通信データをセキュリティサーバ30の透過許容データに擬似的に変換してクライアント30a専用のバッファ領域に蓄積する。クライアント30aから受信要求があったときは、該当するバッファ領域から随時データを読み出してクライアント30a宛に送信する（ステップS307）。このステップS306以降の処理をすべての通信データの送信が終了するまで繰り返す（ステップS308）。

【0024】なお、クライアント30aからクライアント20aへのデータ送信要求は、ステップS201におけるデータ送信要求の主体がクライアント30aに置き換えることで実現することができる。このようにして、リアルタイム通信またはそれに近似した通信が可能になる。

【0025】図6は、本実施形態のデータ通信システムにおいて、あるセキュリティサーバAの配下にあるクライアントAから他のセキュリティサーバBの配下にあるクライアントBへのデータ通信が、どのような手順で実行されるかを全体的な流れで示したシーケンスチャートである。ここでは、セキュリティサーバAの透過許容データがHTTPデータ、セキュリティサーバBの透過許容データがSMTPデータであるものとする。リレーサーバは、上述のリレーサーバ10である。

【0026】クライアントAからクライアントBへのセッション確立が要求されると（A11）、リレーサーバ10はその可否を判断し、その結果をクライアントAへ通知する（C11）。セッション確立が許可された場合、クライアントAは、通信データをエンコードし（A12）、そのヘッダ部に、通信データがHTTP形式であり且つクライアントB宛の返信データである旨の情報を付加してデータ送信要求を発行する（A13）。

【0027】セキュリティサーバAは、通信データのヘッダ部から該通信データが透過許容データであるかどうかを審査する。肯定的であれば、リレーサーバ10に当該通信データを送信する（B11）。通信データを受信したリレーサーバ10は、該通信データをクライアントB専用のバッファ領域に通信データを格納し（C12）、さらに、クライアントBに対して送信可能なデータがあることを通知する。

【0028】通知を受けたクライアントBは、リレーサーバ10にデータ受信要求を発行する（F11）。このデータ受信要求を受け付けたリレーサーバ10は、クライアントB専用のバッファ領域に記憶されているデータをエンコードし、そのヘッダ部に当該データがクライアントBの要求に応じて返信するデータである旨の情報と、当該データがSMTP形式である旨の情報を付加し（C14）、これをセキュリティサーバBに送信する（C15）。

【0029】セキュリティサーバBは、リレーサーバ10から送信されてきた通信データのヘッダ部を審査して

該通信データが透過許容データ、つまりクライアントBの要求した返信データであり且つSMTP形式であることを確認した後、クライアントBに、その通信データを転送する(D11)。クライアントBは、その通信データの受信を完了した後、各処理に移行する。

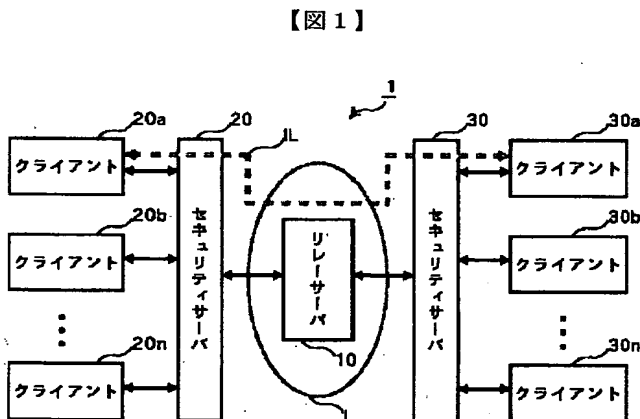
【0030】このようにして、インターネット上でそれぞれ独立のセキュリティサーバの配下にある2台以上のクライアントについて、セキュリティサーバ及び回線の性能限界範囲でのリアルタイム通信を行うことが可能になる。このようなデータ通信の形態は、インターネットを通じて対戦できる対戦型ゲームサービスやリアルタイムチャットサービス等に広く適用することが可能となる。

【0031】

【発明の効果】以上の説明から明らかなように、本発明によれば、相手側との間の直接的なデータ通信が制限される環境下においてもリアルタイム通信乃至それに近似した通信を行うことができるという、特有の効果がある。

【図面の簡単な説明】

【図1】本発明を適用したデータ通信システムの構成図。



【図2】本実施形態によるリレーサーバの機能ブロック構成図。

【図3】本実施形態によるリレーサーバへの登録処理手順図。

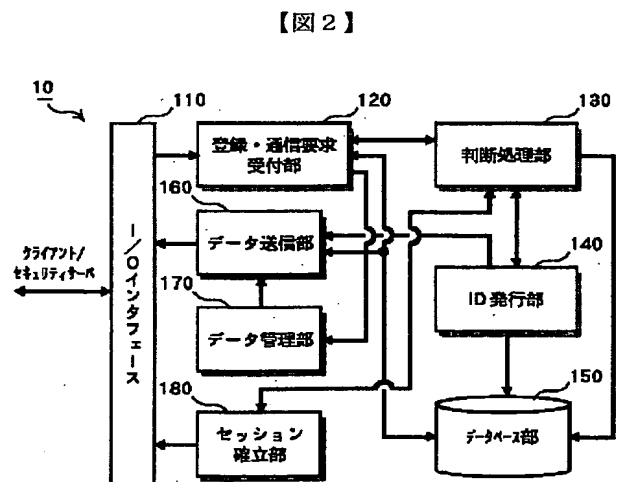
【図4】本実施形態によるクライアント間のデータ通信の処理手順図。

【図5】本実施形態によるクライアント間のデータ通信の処理手順図。

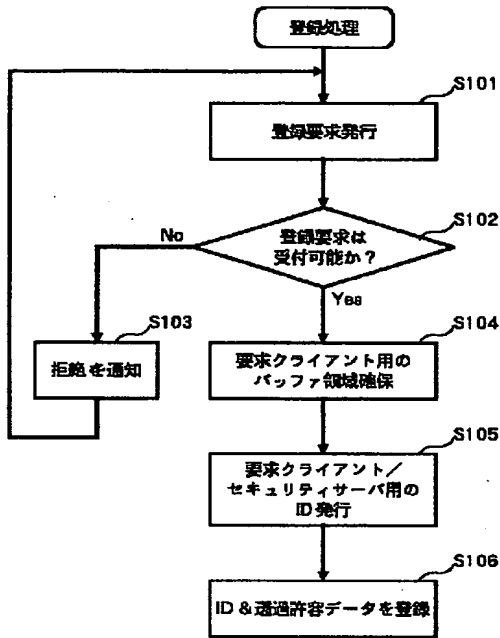
【図6】全体的なデータ通信の処理の流れを示したシーケンスチャート。

【符号の説明】

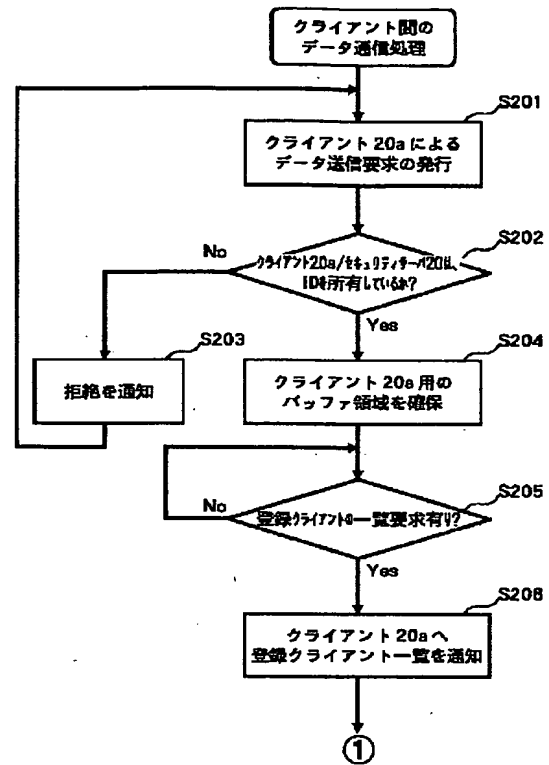
- 1 データ通信システム
- 10 リレーサーバ
- 110 I/Oインターフェース
- 120 登録・通信要求部
- 130 判断処理部
- 140 ID発行部
- 150 データベース部
- 160 データ送信部
- 170 データ管理部
- 180 セッション確立部



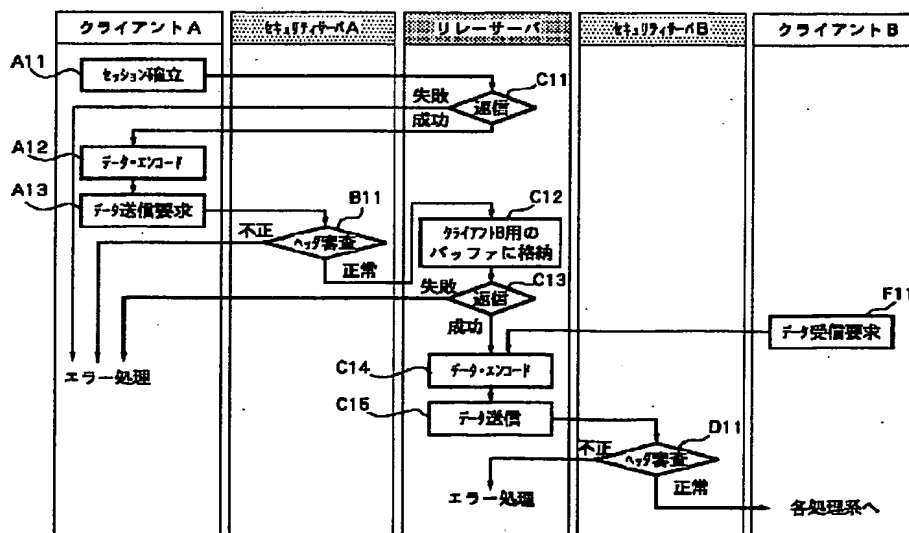
【図 3】



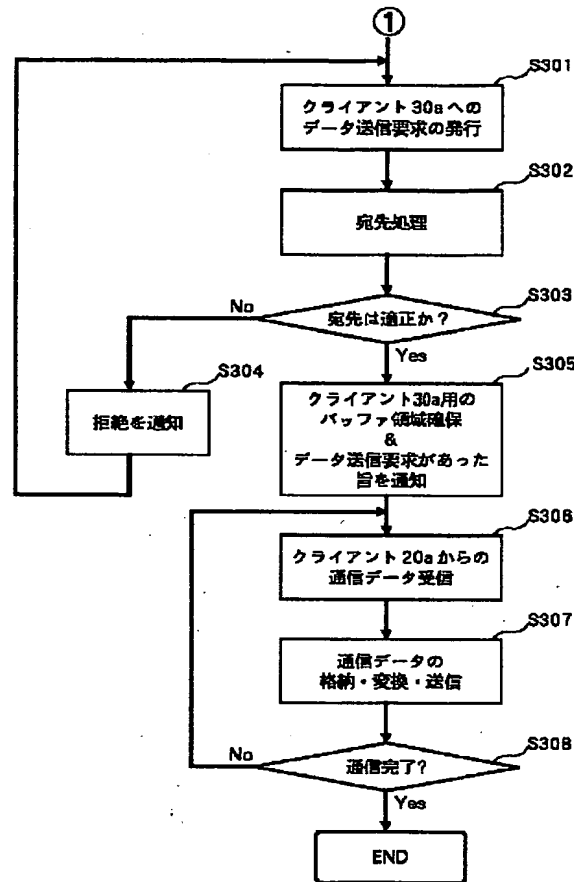
【図 4】



【図 6】



【図 5】



【手続補正書】

【提出日】平成11年8月27日(1999. 8. 27)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 配下にある1又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、前記セキュリティ装置と外部装置との間にデータ中継装置を介在させ、このデータ中継装置で、外部装置から特定の前記通信装置宛の適正なIDが付された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする、データ通信方法。

【請求項2】 前記外部装置、セキュリティ装置及び前

記特定の通信装置をそれぞれ登録しておき、登録された外部装置から登録された通信装置宛の通信データのみを前記透過許容データに擬似的に変換して前記登録されたセキュリティ装置を透過させることを特徴とする、請求項1記載のデータ通信方法。

【請求項3】 それぞれ配下にある1又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容する複数のセキュリティ装置が介在する環境で行うデータ通信方法であって、一のセキュリティ装置と他のセキュリティ装置との間にデータ中継装置を介在させ、このデータ中継装置で、一のセキュリティ装置の配下にある第1通信装置から他のセキュリティ装置の配下にある第2通信装置宛の適正なIDが付された通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させることを特徴とする、データ通信方法。

【請求項4】 前記通信データまたは透過許容データを前記第2通信装置毎に一時的に保持しておき、前記第2

通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、当該透過許容データについてはそれを当該第2通信装置宛に送信することを特徴とする、請求項3記載のデータ通信方法。

【請求項5】 配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在し、前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある相手側通信装置を登録する登録手段と、前記登録された外部装置から前記登録された相手側通信装置宛の通信データを登録された前記セキュリティ装置用の透過許容データに擬似的に変換するデータ変換手段と、前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く手段とを備えて成る、データ中継装置。

【請求項6】 前記相手側通信装置毎のデータ記憶領域を有し、前記通信データ変換手段は、保持されている前記通信データを前記相手側通信装置からの要求を契機に前記透過許容データに擬似的に変換することを特徴とする、請求項5記載のデータ中継装置。

【請求項7】 前記データ変換手段は、前記通信データのヘッダ部分に、当該通信データが前記相手側通信装置からの要求に応じたものであり且つHTTPまたはSMTPに従うデータである旨の情報を付加することで当該通信データを擬似的に前記透過許容データに変換することを特徴とする、請求項6記載のデータ中継装置。

【請求項8】 前記外部装置が、前記セキュリティ装置と同種の機能を有する他のセキュリティ装置の配下にある通信装置であることを特徴とする、請求項5記載のデータ中継装置。

【請求項9】 前記セキュリティ装置及び前記他のセキュリティ装置と共に、TCP/IPに準拠した公衆通信網に接続されることを特徴とする、請求項8記載のデータ中継装置。

【請求項10】 配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも、前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理と、前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理と、前記擬似的に変換された透過許容データを前記セキュリ

ティ装置を介して前記登録された相手側通信装置に導く処理とを実行させるためのプログラムが記録された、コンピュータ読取可能な記録媒体。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0005

【補正方法】変更

【補正内容】

【0005】

【課題を解決するための手段】上記課題を解決する本発明のデータ通信方法は、配下にある1又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、セキュリティ装置と外部装置との間にデータ中継装置を介在させ、このデータ中継装置で、外部装置から特定の前記通信装置宛の適正なIDが付された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする。好ましくは、前記セキュリティ装置及び前記特定の通信装置を予め登録しておき、登録した通信装置宛の通信データのみを前記透過許容データに擬似的に変換して登録されたセキュリティ装置を透過させるようにする。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正内容】

【0006】前記セキュリティ装置が複数介在する環境でデータ通信を行う場合は、前記データ中継装置をセキュリティ装置間に介在させ、特定のセキュリティ装置の配下にある第1通信装置から他のセキュリティ装置の配下にある第2通信装置宛の適正なIDが付された通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させる。なお、前記通信データまたは透過許容データを前記第2通信装置毎に一時的に保持しておき、前記第2通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、前記透過許容データについてはそれを当該第2通信装置宛に送信するようにしてもよい。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0007

【補正方法】変更

【補正内容】

【0007】上記他の課題を解決する本発明のデータ中継装置は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在するもので、前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある

相手側通信装置を登録する登録手段と、前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に登録された前記セキュリティ装置用の透過許容データに変換するデータ変換手段と、前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く手段とを備えて構成したものである。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正内容】

【0009】上記他の課題を解決する本発明の記録媒体は、配下にある通信装置との間で所定形態の透過許容デ

ータのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも下記の処理を実行させるためのプログラムが記録された、コンピュータ読取可能な記録媒体である。

(1) 前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理、

(2) 前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理、

(3) 前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く処理。

フロントページの続き

(72)発明者 川上 量生
東京都中央区日本橋人形町2丁目13番9号
BR人形町1ビル3階 株式会社ダウン
ゴ内

Fターム(参考) 5K030 GA15 HA05 HD01 JT02 LC13
LD19 LD20
9A001 LL03

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.